

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SATO
SERIAL NO: NEW APPLICATION
FILED: HEREWITH
FOR: NON-CONTACT IC CARD

GAU:
EXAMINER:

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

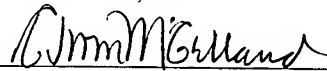
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-236944	August 15, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier

Registration No. 25,599

C. Irvin McClelland
Registration Number 21,124



22850

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月15日

出 願 番 号

Application Number:

特願2002-236944

[ST.10/C]:

[JP2002-236944]

出 願 人

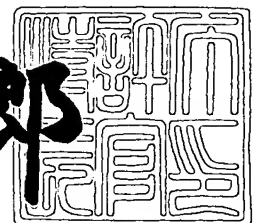
Applicant(s):

ソニー株式会社

2003年 6月10日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3044926

【書類名】 特許願

【整理番号】 0290074301

【提出日】 平成14年 8月15日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00
H04L 9/30
H04L 9/06
H04B 1/38
G06K 19/07

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 佐藤 英雄

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100110434

【弁理士】

【氏名又は名称】 佐藤 勝

【手数料の表示】

【予納台帳番号】 076186

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0011610

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 非接触式 I C カード

【特許請求の範囲】

【請求項 1】 リーダライタとの間のデータの授受を、該リーダライタと接触せずに行う非接触式 I C カードにおいて、

公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理部と、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理部とを有する暗号化手段と、

上記リーダライタとの通信処理と、上記暗号化手段での暗号化処理とにおける動作周波数を変化させる周波数制御手段とを備えることを特徴とする非接触式 I C カード。

【請求項 2】 上記暗号化手段においては、公開鍵暗号化方式による暗号化処理時には、公開鍵暗号化方式による暗号化処理に使用しないハードウェアの動作を停止させ、共通鍵暗号化方式による暗号化処理時には、共通鍵暗号化方式による暗号化処理に使用しないハードウェアの動作を停止させることを特徴とする請求項 1 記載の非接触式 I C カード。

【請求項 3】 上記公開鍵暗号化処理部と上記共通鍵暗号化処理部とは、機能的に共通するハードウェアを共有し、処理モードに応じて、ハードウェアを時分割に切り替えて動作させることを特徴とする請求項 1 記載の非接触式 I C カード。

【請求項 4】 クロックギアにより上記動作周波数を変化させることを特徴とする請求項 1 記載の非接触式 I C カード。

【請求項 5】 分周器により上記動作周波数を変化させることを特徴とする請求項 1 記載の非接触式 I C カード。

【請求項 6】 イネーブル信号のデューティを制御して上記動作周波数を変化させることを特徴とする請求項 1 記載の非接触式 I C カード。

【請求項 7】 リーダライタからの制御信号により上記動作周波数を変化させることを特徴とする請求項 1 記載の非接触式 I C カード。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、リーダライタとの間で、非接触でデータの授受が可能な非接触式 I C カードに関する。

【0 0 0 2】

【従来の技術】

近年、いわゆるインターネット等を利用した電子商取引やオンラインショッピングといった各種通信技術を利用した様々なサービスが普及しつつある。また、通信技術の進歩にともない、端末を介した通信技術のみならず、例えば、交通機関の料金徴収やいわゆる電子マネー等に利用するための通信機能を集積回路化した非接触式半導体メモリカードといったカード状のデバイス（以下、非接触式 I C (Integrated Circuit) カードという。）も開発されている。このような非接触式 I C カードは、取り扱いの便宜等の観点から、少ない回路規模で構成されるとともに、極めて少ない電力消費で動作するように構成される必要がある。

【0 0 0 3】

ところで、上述した非接触式 I C カードを用いたサービスにおいては、通常、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理が行われる。その際、非接触式 I C カードにおいては処理の高速化が要求されるが、これらの機能をソフトウェアによって実装すると、高いクロックの C P U (Central Processing Unit) を要することとなり、実用的でない。そのため、非接触式 I C カードにおいては、上述した相互認証処理や暗号化処理の機能をソフトウェアによって実装するのではなく、ハードウェアによって実装することが望ましい。

【0 0 0 4】

ここで、このようなハードウェアによって上述した機能を実装する非接触式 I C カードにおいては、電力消費を極力抑制するために、例えばいわゆる D E S (Data Encryption Standard) 暗号化方式等の比較的少ない回路規模及び電力消費で実装することができるいわゆる共通鍵暗号化方式を採用するものが多かった。このような共通鍵暗号化方式を採用する非接触式 I C カードにあっては、一般的に、リーダライタとの通信距離が数センチのものが実現されており、インターフ

エースのタイプによっては10cmの通信距離を実現しているものもある。

【0005】

しかしながら、暗号化及び復号に共通の鍵を用いる共通鍵暗号化方式は、鍵データの授受を行う必要があるといった観点から、不正な第三者による攻撃に弱いという問題がある。そのため、非接触式ICカードにおいては、将来的に金融サービスに適用する場合等の問題が懸念されていた。

【0006】

そのため、非接触式ICカードを用いたサービスにおいては、例えばいわゆるRSA (Rivest-Shamir-Adleman) 暗号化方式や楕円曲線暗号化方式 (Elliptic Curve Cryptosystem; ECC) といったように、暗号化と復号とに用いる鍵を異なるものとし、秘密に保つ必要がある共通鍵を特定の1人が持てばよい、いわゆる公開鍵暗号化方式を採用したセキュリティの高いシステムが要求されつつあり、公開鍵を用いた署名生成及び署名検証を行う非接触式ICカードの開発も多く試みられている。

【0007】

【発明が解決しようとする課題】

しかしながら、公開鍵暗号化方式は、共通鍵暗号化方式に比べ、セキュリティが高く安全性が極めて向上するものの、演算量が非常に膨大となることから、これをハードウェアによって実装する際には、回路規模が数十倍に増大し、規模が増大した回路に供給する電力も必然的に増大することになる。

【0008】

そのため、このような公開鍵暗号化方式を採用した非接触式ICカードにおいては、回路規模、電力消費、及びコストの面で十分な特性を得ることができなかった。特に、非接触式ICカードにおいては、限られた電力の多くを、暗号化処理を行うための回路に供給する必要があることから、通信距離が数ミリ程度と小さいものしか実用化されていないのが実情である。

【0009】

このように、非接触式ICカードにおいては、セキュリティの面で強固であり公開鍵暗号化方式を採用することが期待されているものの、供給可能な電力やチ

ップサイズ等の制限があり、また通信距離も小さく実用に耐えられないことから、実装することが極めて困難であった。

【 0 0 1 0 】

そこで、本発明は、このような実情に鑑みてなされたものであり、公開鍵暗号化方式を採用した場合であっても十分な通信距離を確保し、単一のカードで共通鍵暗号化方式と公開鍵暗号化方式とを両立させ、種々のサービスに適用可能な非接触式 IC カードを提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上述した課題を解決する本発明に係る非接触式 IC カードは、リーダライタとの間のデータの授受を、該リーダライタと接触せずに行うものであり、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理部と、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理部とを有する暗号化手段と、リーダライタとの通信処理と、暗号化手段での暗号化処理とにおける動作周波数を変化させる周波数制御手段とを備えることを特徴とする。

【 0 0 1 2 】

本発明に係る非接触式 IC カードでは、通信処理と暗号化処理とが動作周波数を変更しながらおこなわれる。このような非接触式 IC カードによれば、各種処理毎に異なる動作周波数で当該各種処理を実行する、例えば暗号化処理時にはより低い動作周波数で暗号化手段を動作させることにより、暗号化処理時の瞬時電力が低下し、電力消費が削減される。したがって、本発明では、暗号化方式に公開鍵暗号化方式を採用した場合であっても、リーダライタとの通信に出力する電力がより多く確保され、十分な通信距離を確保することが可能とされ、共通鍵暗号化方式とともに公開鍵暗号化方式を採用する、いわゆる 2 ウェイのカードの実現が容易となる。

【 0 0 1 3 】

また、本発明に係る非接触式 IC カードは、暗号化手段においては、公開鍵暗号化方式による暗号化処理時には、公開鍵暗号化方式による暗号化処理に使用しないハードウェアの動作を停止させ、共通鍵暗号化方式による暗号化処理時には

、共通鍵暗号化方式による暗号化処理に使用しないハードウェアの動作を停止させる。さらに、本発明の非接触式ＩＣカードは、公開鍵暗号化処理部と上記共通鍵暗号化処理部とを、機能的に共通するハードウェアを共有し、処理モードに応じて、ハードウェアを時分割に切り替えて動作させる。

【 0 0 1 4 】

本発明に係る非接触式ＩＣカードは、各処理にて使用し、ハードウェアは動作させず、また、各種処理を行うための各ハードウェアを共有し、時分割に切り換えて動作させる。このような非接触式ＩＣカードによれば、必要なハードウェアのみの動作や、ハードウェアの共有に伴う回路規模の削減により、電力消費がさらに削減され、より２ウェイカードの実現が容易となる。

【 0 0 1 5 】

【発明の実施の形態】

以下、本発明に係る非接触式ＩＣカードの具体的な実施の形態について、図面を参照しながら詳細に説明する。

【 0 0 1 6 】

非接触式ＩＣカード１は、図１（ａ）に示すように、ＩＣモジュール２が一对の熱可塑性樹脂３ａ、３ｂで挟み込まれてなる。ＩＣモジュール２は、同図（ｂ）に示すように、暗号化手段を有するＩＣチップ４と、該ＩＣチップ４に接続され且つデータの授受等、リーダライタとの間で通信を行うためのアンテナコイル等のアンテナ回路５とで構成されている。なお、熱可塑性樹脂３ａ、３ｂの表面には、ＰＶＣ等の樹脂からなる保護層等を設けても良い。

【 0 0 1 7 】

この非接触式ＩＣカード１は、通信機能を集積回路化した非接触式の半導体メモリカードであり、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理の機能が、暗号化手段としてのハードウェア（ＩＣチップ４）によって実装されたものである。特に、この非接触式ＩＣカード１は、共通鍵暗号化方式と公開鍵暗号化方式とをともに採用し、これら各暗号化方式が、提供するサービスに応じて使い分けられるものである。この非接触式ＩＣカード１においては、いずれの暗号化方式が用いられるかは、受信し

たデータのヘッダ情報等により識別される。

【 0 0 1 8 】

この非接触式 I C カード 1 では、I C チップ 4 において、リーダライタとの通信処理を含む各種処理を行うための各ハードウェアが、当該各種処理間で共用され、これら各種処理が時分割して行われる。なお、以下の説明では、便宜上、共通鍵暗号化方式として D E S (Data Encryption Standard) 暗号化方式を採用し、また、公開鍵暗号化方式として、いわゆる楕円曲線暗号化方式 (Elliptic Curve Cryptosystem ; E C C) を採用するものとして説明する。さらに、公開鍵暗号化方式において認証やデジタル署名等に用いるハッシュ関数として、いわゆる S H A - 1 (Secure Hash Algorithm-1) を用い、さらに、公開鍵を用いた暗号化処理を行う際に必要となる鍵生成の過程等で用いる乱数を、上述した D E S 暗号化方式を用いて生成するものとする。すなわち、非接触式 I C カード 1 は、共通鍵暗号化方式の信号処理として D E S 暗号化処理を、公開鍵暗号化方式の一連の信号処理として、少なくとも上述した楕円曲線暗号化処理、S H A - 1 処理、及び D E S 暗号化処理を行うものである。

【 0 0 1 9 】

まず、非接触式 I C カード 1 において、D E S 暗号化処理、楕円曲線暗号化処理及び S H A - 1 処理を行うための各ハードウェアを共用するための概念について説明する。

【 0 0 2 0 】

非接触式 I C カード 1 は、実装される I C チップ 4 において、D E S 暗号化処理、楕円曲線暗号化処理及び S H A - 1 処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用する。すなわち、共通鍵による暗号化処理として、或いは公開鍵による暗号化処理時に乱数生成手段として D E S 暗号化処理を行う暗号化エンジン (D E S 処理回路) におけるハードウェア構成要素は、機能分析的に分解すると、図 2 (a) に概念を示すように、レジスタ群と D E S 演算処理コア回路とに大別することができる。また、楕円曲線暗号化処理を行う暗号化エンジン (楕円曲線処理回路) におけるハードウェア構成要素は、機能分析的に分解すると、同図 (b) に概念を示すように、レジスタ群と楕円曲線演算処

理コア回路とに大別することができ、また、SHA-1 処理を行う暗号化エンジン（SHA-1 処理回路）におけるハードウェア構成要素についても、機能分析的に分解すると、同図（c）に示すように、レジスタ群と SHA-1 演算処理コア回路とに大別することができる。これら各種処理を行うハードウェア構成要素においては、同図（a）乃至（c）に示すように、レジスタ群が当該ハードウェア構成要素の半分程度を占めている。そこで、同図（d）に示すように、DES 暗号化処理、楕円曲線暗号化処理及び SHA-1 処理のそれぞれを行うためのハードウェア構成要素としてのレジスタ群を共用する。これにより、非接触式カード 1 は、IC チップ 4 における暗号化手段の回路規模の削減を図ることが可能となる。

【 0 0 2 1 】

また、上述した非接触式 IC カード 1 においては、SHA-1 処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とを共用する。すなわち、ハッシュ値を算出する SHA-1 処理においては、高速に動作する加算器が設けられた演算処理コア回路が必要とされる。また、楕円曲線暗号化処理においても、演算処理コア回路に加算器が設けられる。そこで、SHA-1 処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とにおける加算器等のゲート数が多いハードウェア構成要素を共用する。これにより、非接触式 IC カード 1 は、IC チップ 4 における暗号化手段の回路規模の削減を図ることが可能となる。

【 0 0 2 2 】

さらに、非接触式 IC カード 1 においては、暗号化エンジンにおけるバス切り替えスイッチ群とその他各種機能の切り替えスイッチとを共用する。すなわち、公開鍵暗号化方式における鍵長を可変とするためにはバスを切り替える必要があることから、楕円曲線暗号化処理を行う暗号化エンジンには、例えば 32 ビット幅のスイッチが多数設けられる。これらのスイッチは、その構成上、SHA-1 処理や DES 暗号化処理を行うハードウェアにおいても共用可能である。そこで、暗号化装置においては、これらバス切り替えスイッチ群を、その他各種機能の切り替えスイッチとして流用する。これにより、非接触式 IC カード 1 は、IC

チップ 4 の暗号化手段の回路規模の削減を図ることが可能となる。

【 0 0 2 3 】

さらにまた、非接触式 IC カード 1 では、IC チップ 4 における上述したレジスタやメモリ等の各ハードウェアが時分割共用される。すなわち、非接触式 IC カード 1 は、リーダライタとの通信後に、共通鍵暗号化方式の信号処理、又は公開鍵暗号化方式の信号処理が行われるが、これら通信、信号処理は、同時には行うことができないものである。したがって、ハードウェアを共用する場合には必然的に時分割処理を行うことになる。そこで、これを利用して、レジスタやメモリ等のハードウェアが各処理で時分割共用される。以下に、上述したようにハードウェアが共有されている非接触式 IC カード 1 における各種処理の時分割処理について説明する。

【 0 0 2 4 】

非接触式 IC カード 1 の IC チップ 4 は、図 3 に示すように、各部を制御する CPU 1 1 と、この CPU 1 1 のワークエリアとして機能するメモリであって、例えば 2 K B 程度の容量を有する RAM 1 2 と、各種プログラム等を記憶する読み出し専用のメモリであって、例えば 3 2 K B 程度の容量を有する ROM 1 3 と、電氣的に書き換え可能とされるメモリであって、例えば 9 K B 程度の容量を有する E E P R O M (Electrically Erasable Programmable Read Only Memory) 1 4 と、電源回路等のアナログブロック 1 5 と、アンテナ回路 5 と接続される無線通信を行うための R F (Radio Frequency) ブロック 1 6 と、D E S 暗号化処理、楕円曲線暗号化処理及び S H A - 1 処理を行う暗号化ブロックである E C C / S H A 1 / D E S ブロック 1 7 と、ハッシュ値を格納するメモリであって、例えば 1 K B 程度の容量を有する A L U R A M (Arithmetic and Logical Unit Random Access Memory) 1 8 と、テスター用のランドからなるテストブロック 1 9 と、CPU 1 1 と各部との間でデータの授受を行うためのバスである CPU インターフェース 2 0 とを集積回路化して構成される。

【 0 0 2 5 】

このような IC チップ 4 を有する非接触式 IC カード 1 は、CPU 1 1 の制御のもとに、E C C / S H A 1 / D E S ブロック 1 7 を動作させ、共通鍵を用いた

暗号化処理としてDES暗号化処理を、公開鍵を用いた暗号化処理として楕円曲線暗号化処理、SHA-1処理、及びDES暗号化処理を行う。この非接触式ICカード1における処理モードは、主に、リーダライタとの通信を行う通信モード、楕円曲線暗号化処理を行う楕円曲線暗号化処理モード、DES暗号化処理を行うDES暗号化処理モード、及びALU RAM18に対してアクセスするALU RAMモードの4つに大別される。そして、非接触式ICカード1では、各処理モードに応じて、動作させるハードウェアを時分割に切り替える。

【0026】

非接触式ICカード1における時分割動作を具体的に説明するために、まず、図4に示すように、各部を機能的に表現する。なお、同図においては、アナログブロック15については図示を省略するとともに、説明の便宜上、ECC/SHA1/DESブロック17を、楕円曲線暗号化処理及びSHA-1処理の機能を表すECC/SHA1ブロック17₁と、DES暗号化処理の機能を表すDESブロック17₂とに大別して表現している。

【0027】

非接触式ICカード1においては、通信モード時には、図5(a)中太線枠で示すように、CPU11、RAM12、ROM13、EEPROM14、及びRFブロック16のみが動作する。すなわち、非接触式ICカード1においては、通信モード時には、CPU11の制御のもとに、ROM13に記憶されている所定の通信プログラムが起動し、RAM13やEEPROM14に記憶されている各種情報が、RFブロック16を介して外部に送信されるとともに、RFブロック16を介して外部から受信した各種情報が、RAM13やEEPROM14に記憶される。そして、この通信モードでは、通信モード時に不要な暗号化ブロック、すなわちECC/SHA1ブロック17₁とDESブロック17₂、ALU RAM18が動作しないよう制御される。このような通信モードにおける各ハードウェアの動作、具体的には暗号化ブロックの停止は、各ハードウェアを各種処理において共有し、これら各種処理を時分割で行うことによって可能となる。

【0028】

また、非接触式ICカード1においては、DES暗号化処理モード時には、同

図（b）中太線枠で示すように、CPU 1 1、RAM 1 2、ROM 1 3、及びDESブロック1 7₂が動作する。すなわち、非接触式ICカード1においては、DES暗号化処理モード時には、CPU 1 1の制御のもとに、ROM 1 3に記憶されている所定の擬似乱数（Pseudo-random Number；以下、PNという。）系列がシード（seed）や鍵データとして読み出され、RAM 1 2がワークエリアとして用いられながら、DESブロック1 7₂によってDES暗号化処理が行われる。そして、このDES暗号化処理モードでは、DES暗号化処理に不要な暗号化ブロック、すなわちECC／SHA1ブロック1 7₁とALU RAM 1 8とが動作しないよう、具体的にはDES暗号化処理に不要なゲートが故意に停止されるよう制御される。このとき、ECC／SHA1ブロック1 7₁の公開鍵暗号化処理用の演算器には、例えば入力値をホールドする、又は入力値を全て「0」又は「1」にする等して、ECC／SHA1ブロック1 7₁を動作しないよう制御する。

【0 0 2 9】

さらに、非接触式ICカード1においては、楕円曲線暗号化処理モード時には、同図（c）中太線枠で示すように、ECC／SHA1ブロック1 7₁及びALU RAM 1 8が動作する。すなわち、非接触式ICカード1においては、楕円曲線暗号化処理モード時には、ECC／SHA1ブロック1 7₁によってSHA-1処理が行われ、得られたハッシュ値がALU RAM 1 8に格納されるとともに、このハッシュ値がALU RAM 1 8から読み出され、このハッシュ値を用いてECC／SHA1ブロック1 7₁によって楕円曲線暗号化処理が行われる。そして、このDES暗号化処理モードでは、DES暗号化処理に不要な暗号化ブロック、すなわちDESブロック1 7₂が動作しないよう、具体的には楕円曲線暗号化処理に不要なゲートが故意に停止されるよう制御される。

【0 0 3 0】

さらにまた、非接触式ICカード1においては、ALU RAMモード時には、同図（d）中太線枠で示すように、CPU 1 1、RAM 1 2、ROM 1 3、及びALU RAM 1 8が動作する。すなわち、非接触式ICカード1においては、ALU RAMモード時には、CPU 1 1の制御のもとに、ROM 1 3に記憶

されている所定の各種情報が読み出され、RAM 1 2 がワークエリアとして用いられながら、ALU RAM 1 8 に対するアクセスが行われる。

【 0 0 3 1 】

このように、非接触式 IC カード 1 においては、SHA-1 処理回路、楕円曲線暗号化処理回路、及び DES 暗号化処理回路における各部を共用し、同時には行うことができない複数の処理を、各処理モードに応じて動作させるハードウェアを時分割に切り替え、使用しないハードウェアの動作を停止状態とすることによって、本来必要とされるゲート数の約 1 / 2 程度のゲート数にまで IC チップ 4 に実装された暗号化手段の回路規模を削減し、また、暗号化処理時等の瞬時電力を大幅に削減して電力消費も約 1 / 2 程度にまで削減することができる。特に、非接触式 IC カード 1 においては、上述したハードウェアの共有化によってゲート数が本来の 1 / 2 に抑えられているため、電力消費の削減も効率的となる。そして、非接触式 IC カード 1 においては、このような電力消費の削減によって、リーダライタとの通信に利用できる電力を上げることができ、公開鍵暗号化処理においても、共通鍵を用いた暗号化処理の場合と同様な通信距離、具体的には数センチメートルもの実用的な通信距離を実現することができるようになる。さらに、非接触式 IC カード 1 は、公開鍵暗号化方式を採用していることから、改竄等の攻撃に対する耐性にも優れ、高い安全性が要求されるサービスに適用して有効である。

【 0 0 3 2 】

また、上述した非接触式 IC カード 1 においては、CPU 1 1 の制御により、時分割で行われる各種処理毎に動作周波数が変更される。したがって、非接触式 IC カード 1 では、通信処理において通信の高速化を保ち得るような動作周波数で動作させ、通信処理に次いで行われる暗号化処理において演算速度を緩める、すなわち暗号化処理時における動作周波数をクロックダウンさせて動作させることができる。このような暗号化処理時にクロックダウンすることにより、非接触式 IC カード 1 では、暗号化処理時等の瞬時電力を大幅に削減して電力消費をさらに低く抑えることができ、リーダライタとの通信に利用できる電力を上げて、公開鍵暗号化の使用における通信距離をより大きくすることが、具体的には 1 0

c m程の通信距離を確保することが可能とされる。

【 0 0 3 3 】

このような非接触式 I C カード 1 は、図 6 に示すように、C P U 1 1 が内蔵するクロックギア 2 1 によって自身でクロックの分周比を選択して、動作周波数を変えることができるよう構成されている。クロックギア 2 1 は、C P U 1 1 からの制御信号により、分周比が、例えば $1/4$ 、 $1/8$ 、 $1/16$ のうちから選択可能とされ、各処理における動作周波数を変更して、暗号化ブロック、すなわち ECC / S H A 1 / D E S ブロック 1 7 を動作させる。例えば、公開鍵を用いた暗号処理が行われる場合、R F ブロック 1 6 及び通信回路 2 2 を介してリーダライタとデータの授受を行う通信処理時には、共通鍵を用いた場合と同じ通信レートとすることができる $1/4$ の分周比を選択し、公開鍵を用いた暗号化処理時には、C P U 1 1 からの制御信号により $1/8$ の分周比を選択することによって、全体的な電力消費を $1/2$ に下げることができる。この場合、暗号化処理の処理時間は分周比を下げる前の 2 倍になってしまうが、暗号化処理時の電力消費が削減されているため、リーダライタとの通信に利用できる電力を上げることができ、共通鍵を用いた暗号化処理と同等の通信距離を確保することができるようになる。非接触式 I C カード 1 の I C チップ 4 では、楕円暗号 1 6 0 ビット (R S A 1 0 2 4 ビット) を 0 . 2 秒程度で署名生成できるため、暗号化処理時の動作周波数を上述した動作周波数にクロックダウンしても十分に実用性は確保することができる。そして、暗号化処理が終了した場合には、再び C P U 1 1 からの制御信号によって、 $1/4$ の分周比を選択することによって、通信レートを維持し、通信の高速化を図ることができる。このように、非接触式 I C カード 1 では、通信レートを変更することなく、すなわち通信の高速化を図りつつ、共通鍵暗号化方式の場合と公開鍵暗号化方式の場合とで同等の通信距離を確保することができる。

【 0 0 3 4 】

なお、上述した例では、暗号化処理時の分周比のみを選択するようにしているが、提供するサービスの種類によっては、暗号化処理時だけでなく通信処理時の分周比も低くなるよう選択し、通信レートを下げることによってさらに通信距離

を大きくするようにしてもよい。

【 0 0 3 5 】

また、非接触式 I C カード 1 においては、リーダライタの種類によって公開鍵を使用した暗号化処理時の動作周波数が変化するようにしてもよい。

【 0 0 3 6 】

例えば、非接触式 I C カード 1 との通信で使用し得る電波の強度は民生機器とライセンスを受けた業務用とは異なる。具体的には、電車の自動改札機といった用途では、非常に強い電波を使用することができるため、十分に大きなリーダライタと非接触式 I C カード 1 との通信距離を確保することができるが、ライセンスを必要としない家庭用のリーダライタにおいては微弱な電波しか使用することができないため、通信距離は小さくなり十分な距離が確保できなくなる。このとき、自動改札機等の業務用のリーダライタは、高速の計算を要するものであるが、上述したように強い電波にて既に十分な通信距離を確保し得る。したがって、通信距離確保のためのクロックダウンの必要が無く、より早く暗号化処理を行うように早い動作周波数となるような分周比を選択するようにクロックギア 2 1 を制御することが好ましい。これとは逆に、家庭用のリーダライタでは、非接触といっても至近距離において、且つ暗号化処理に時間がかかっても良い。したがって、電力消費を低く抑えるためにクロックダウンを行い、遅い動作周波数となる分周比を選択するようにクロックギア 2 1 を制御することが好ましい。このように、提供するサービス毎、具体的には各サービスにて使用するリーダライタ毎に、クロックギア 2 1 にて選択される分周比を制御することによって、1 枚のカードで、上述したようなリーダライタの種類を含む各サービスに必要な状況に応じて各サービスを最適に提供することができるようになる。なお、リーダライタ側から予め高速の暗号化処理又は低速の暗号化処理のいずれを行うかを決定する制御信号を通信処理時データとともに送信する必要がある。

【 0 0 3 7 】

また、このようなクロックギア 2 1 の制御を、非接触式 I C カード 1 側にて自動的に行うよう構成してもよい。このような場合には、電源回路の電圧やポーリング時の同期信号の種類等に従って暗号化処理における動作周波数を決定する。

なお、非接触式 I C カード 1 における安定した動作や、速度、確実性を選ぶなら制御信号をリーダライタ側から送信することが好ましい。

【 0 0 3 8 】

さらに、非接触式 I C カード 1 は、C P U 1 1 がクロックギア 2 1 を内蔵していない場合等、上述したようにクロックギア 2 1 により暗号ブロックの動作周波数を選択するようにしなくとも、例えば図 7 に示すように、分周器 2 3 を介して暗号ブロックに入力する動作周波数についての分周比は変更せずに、イネーブル発生回路 2 4 を設け、イネーブル信号のデューティのみを、サービスを示すコードを送る C P U 1 1 からの各制御信号により制御されるイネーブル発生回路 2 4 によって変更するよう構成しても、また、図 8 に示すように、各サービスを示すコードを送る C P U 1 1 からの制御信号が入力され、該制御信号に応じた動作周波数を暗号化ブロックに入力するクロック分周器 2 5 を設けることにより、暗号ブロックに入力される動作周波数そのものを変化させるよう構成してもよい。このように非接触式 I C カード 1 を構成しても、各ブロックを安定して動作させ、且つ電力消費を削減することができる。

【 0 0 3 9 】

このように、非接触式 I C カード 1 では、各種処理を行うための各ハードウェアを共有、具体的には時分割共有され、且つ動作周波数を変更しながら各種処理がおこなわれる。そして、このようなハードウェアの共有により暗号化手段の回路規模の削減とともに電力消費の削減を図ることができ、また、上述した時分割処理により可能となった各種処理毎に異なる動作周波数での当該各種処理の実行により、さらなる電力消費の削減を図ることができる。その結果、暗号化方式に公開鍵暗号化方式を採用した場合であっても、リーダライタとの通信に出力する電力をより多くすることができ、十分な通信距離を確保することができるようになる。したがって、非接触式 I C カード 1 では、共通鍵暗号化方式とともに公開鍵暗号化方式を採用する、いわゆる 2 ウェイのカードの実現が容易になり、これら 2 種の暗号化方式による種々のサービスを提供することができるようになる。

【 0 0 4 0 】

なお、上述した実施の形態においては、公開鍵暗号化方式として楕円曲線暗号

化方式を使用する場合について説明したが、本発明はこれに限定されるものではなく、R S A等、他の公開鍵暗号化方式を使用するものであってもよい。

【0041】

また、上述した実施の形態では、ハッシュ関数として、S H A - 1を用いるものとして説明したが、本発明は、例えばM D 5 (Message Digest 5) 等の他のハッシュ関数にも容易に適用することができる。

【0042】

さらに、上述した実施の形態では、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の1つであるD E S暗号化方式を用いて生成するものとして説明したが、本発明は、乱数生成の手法については、任意のものを適用することができる。

【0043】

このように本発明は、上述した構成例に限定されるものではなく、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【0044】

【発明の効果】

以上、詳細に説明したように本発明に係る非接触式I Cカードによれば、各種処理毎に異なる動作周波数で当該各種処理を実行する、具体的には暗号化処理時により低い動作周波数で暗号化手段を動作させることにより、電力消費を削減することができる。したがって、本発明では、暗号化方式に公開鍵暗号化方式を採用した場合であっても、リーダライタとの通信に出力する電力をより多く確保でき、リーダライタとの十分な通信距離を確保することできるようになり、共通鍵暗号化方式とともに公開鍵暗号化方式を採用する、いわゆる2ウェイのカードを容易に実現することができる。

【図面の簡単な説明】

【図1】

本実施の形態に係る非接触式I Cカードの構成を説明するための図であり、(a)は縦断面図、(b)はI Cモジュールの配設状態を示す平面図である。

【図2】

ＩＣチップにおける暗号化手段を概念的に説明するための図である。

【図 3】

同非接触式ＩＣカードのＩＣチップの構成を説明するブロック図である。

【図 4】

同非接触式ＩＣカードのＩＣチップにおける各部を機能的に表現したブロック図である。

【図 5】

同非接触式ＩＣカードにおける時分割動作を説明するための図であり、（a）は、通信モード時における動作を説明するためのブロック図であり、（b）は、DES暗号化処理モード時における動作を説明するためのブロック図であり、（c）は、楕円曲線暗号化処理モード時における動作を説明するためのブロック図であり、（d）は、ALU RAMモード時における動作を説明するためのブロック図である。

【図 6】

同非接触式ＩＣカードにおいて、クロックギアにより動作周波数を変化させる動作を説明するためのブロック図である。

【図 7】

同非接触式ＩＣカードにおいて、イネーブル発生器によりイネーブル信号のデューティを変化させる動作を説明するためのブロック図である。

【図 8】

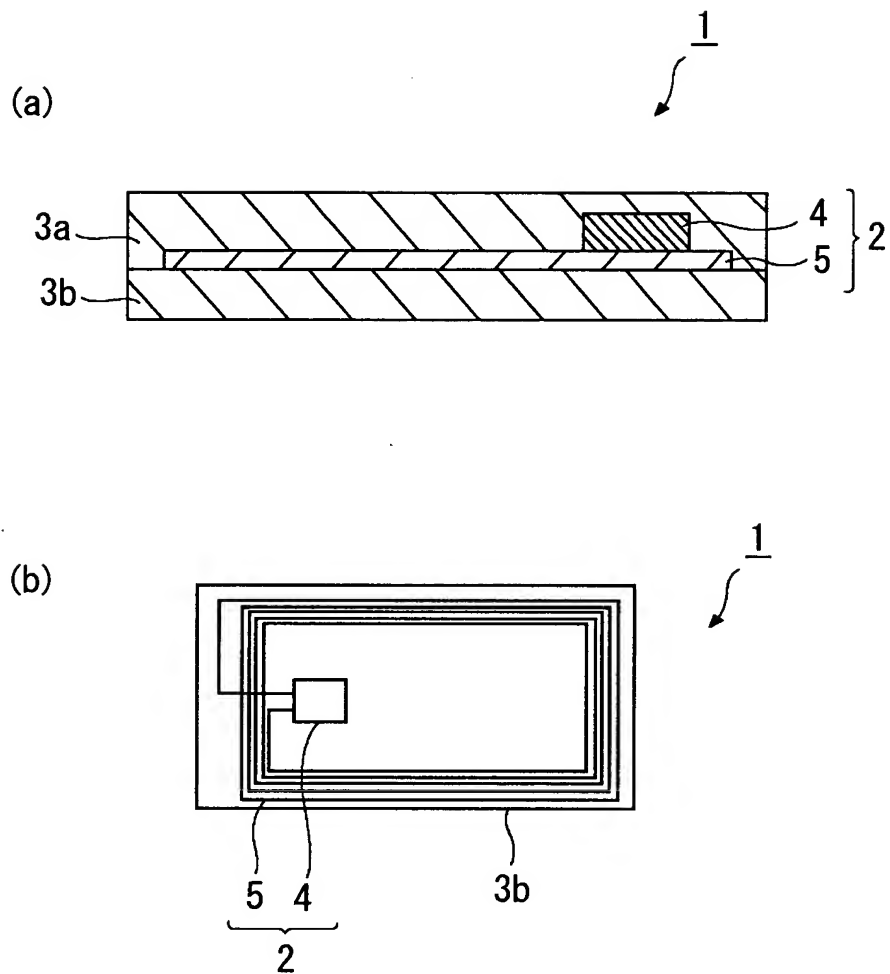
同非接触式ＩＣカードにおいて、クロック分周器により動作周波数を変化させる動作を説明するためのブロック図である。

【符号の説明】

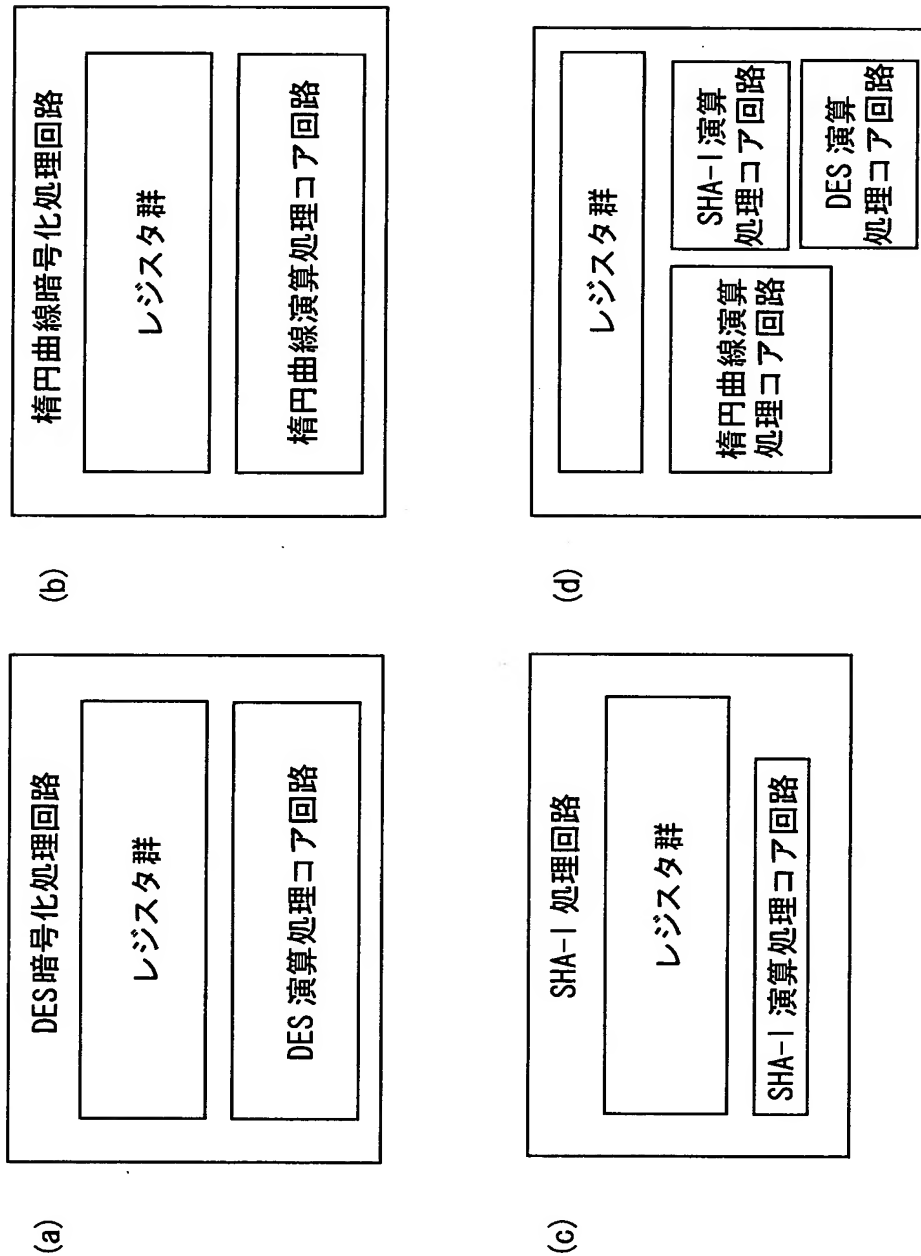
1 非接触式ＩＣカード, 2 ICモジュール, 3 a、3 b 熱可塑性樹脂,
4 ICチップ, 5 アンテナ回路, 11 CPU, 12 RAM, 13 ROM,
14 EEPROM, 15 アナログブロック, 16 RFブロック, 17
ECC/SHA1/DESブロック, 18 ALU RAM, 19 テストブ
ロック, 20 CPUインターフェース, 21 クロックギア, 22 通信回路
, 23 分周器, 24 イネーブル発生器, 25 クロック分周器

【書類名】 図面

【図 1】

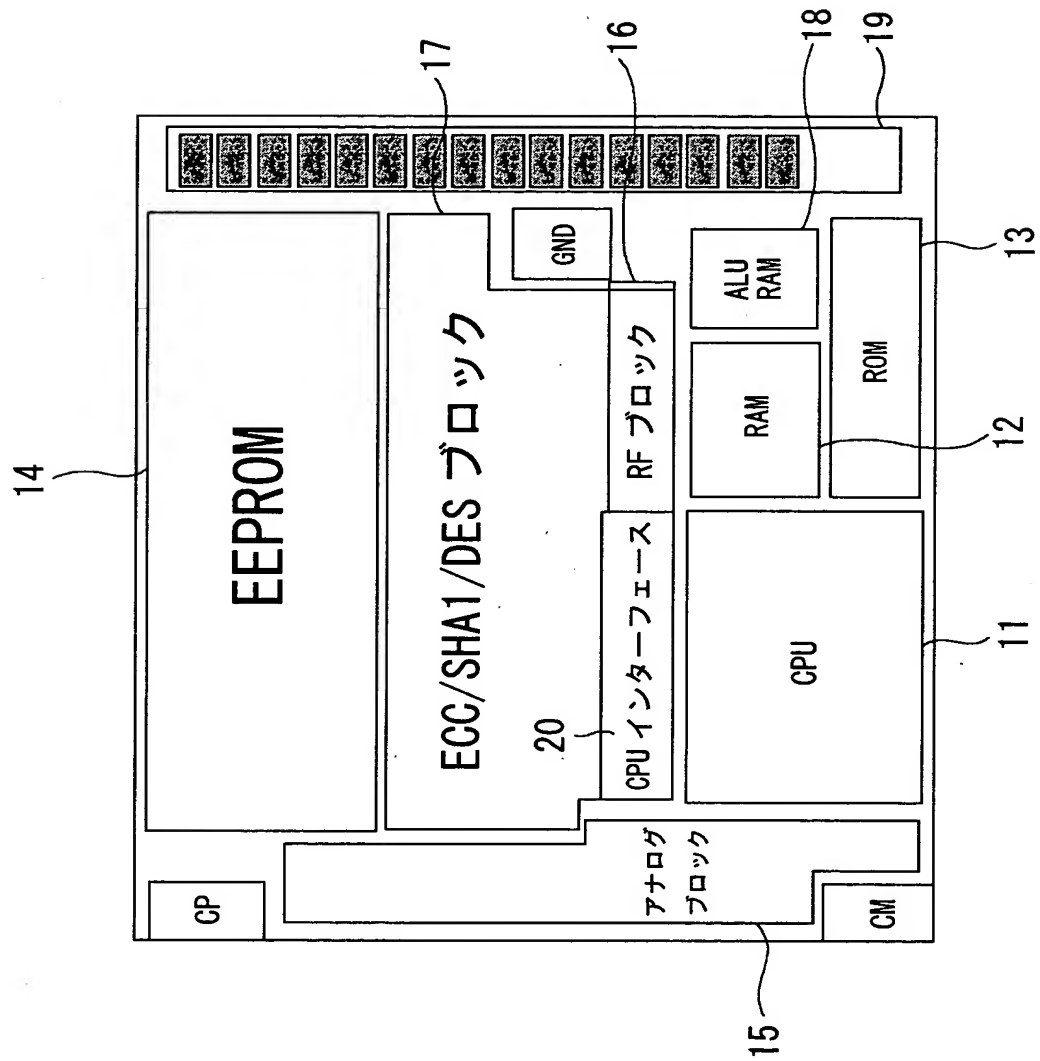


【図 2】



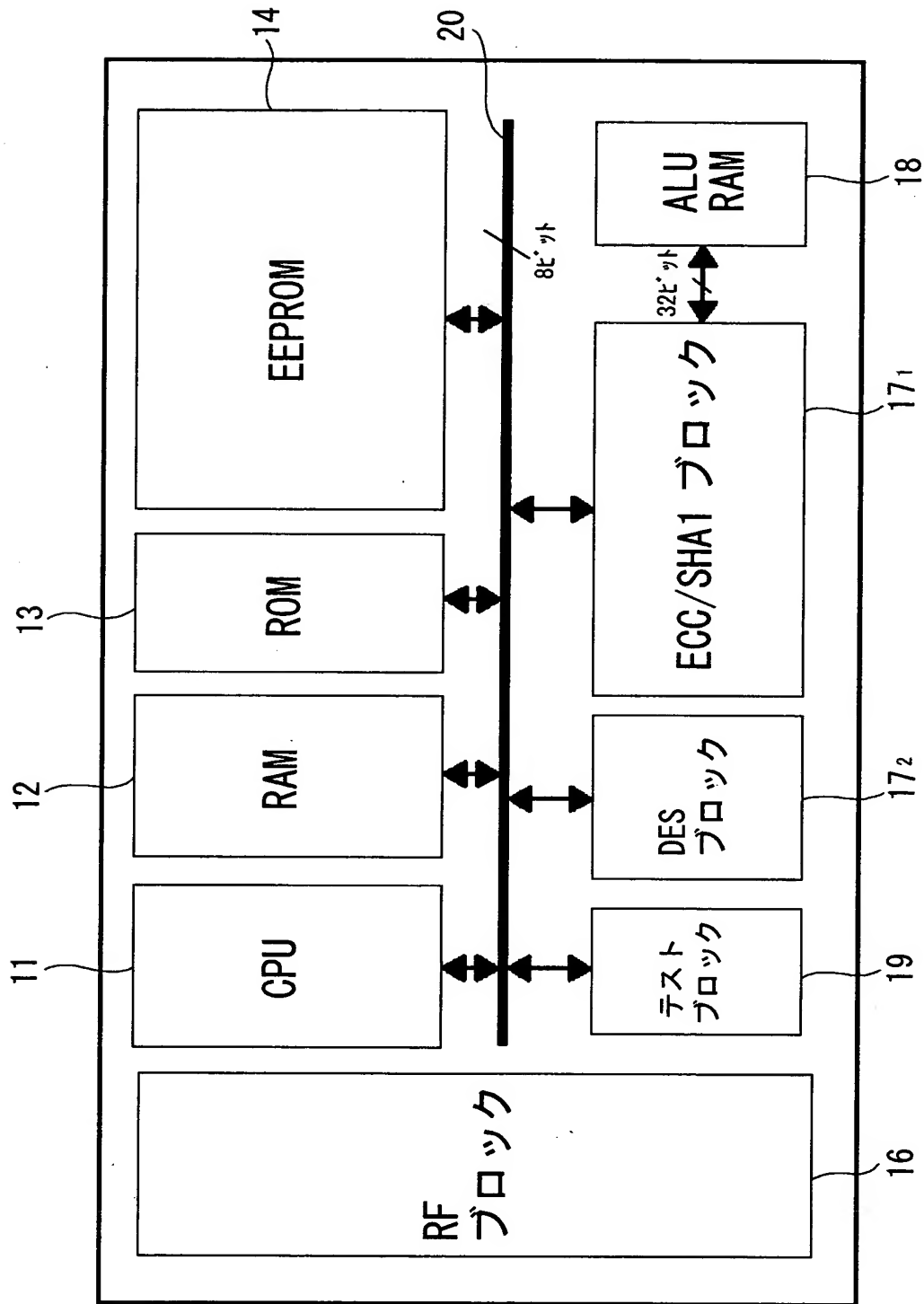
暗号化手段 (IC チップ) の概念図

【図 3】



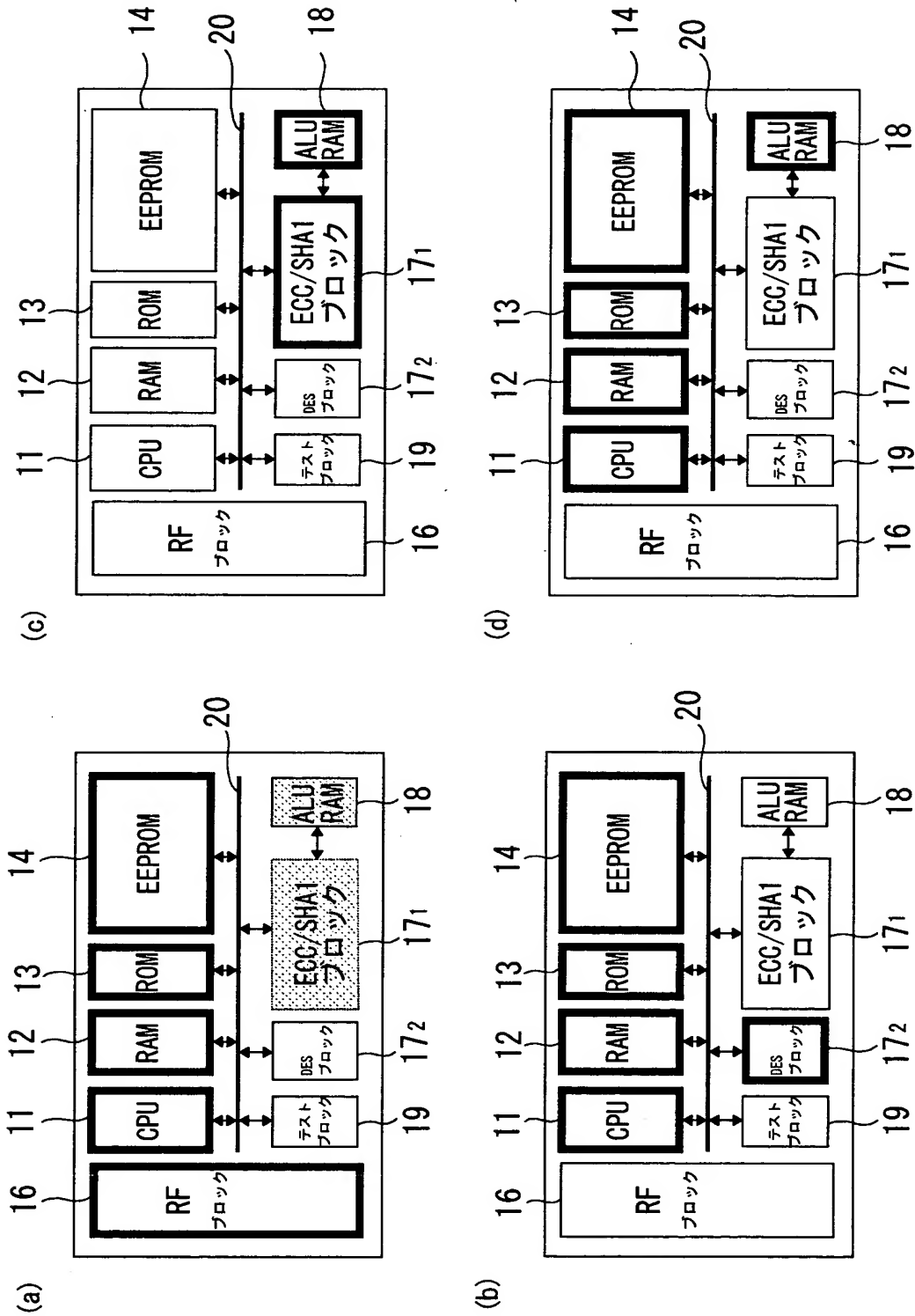
非接触式 IC カードの IC チップの構成ブロック図

【図4】



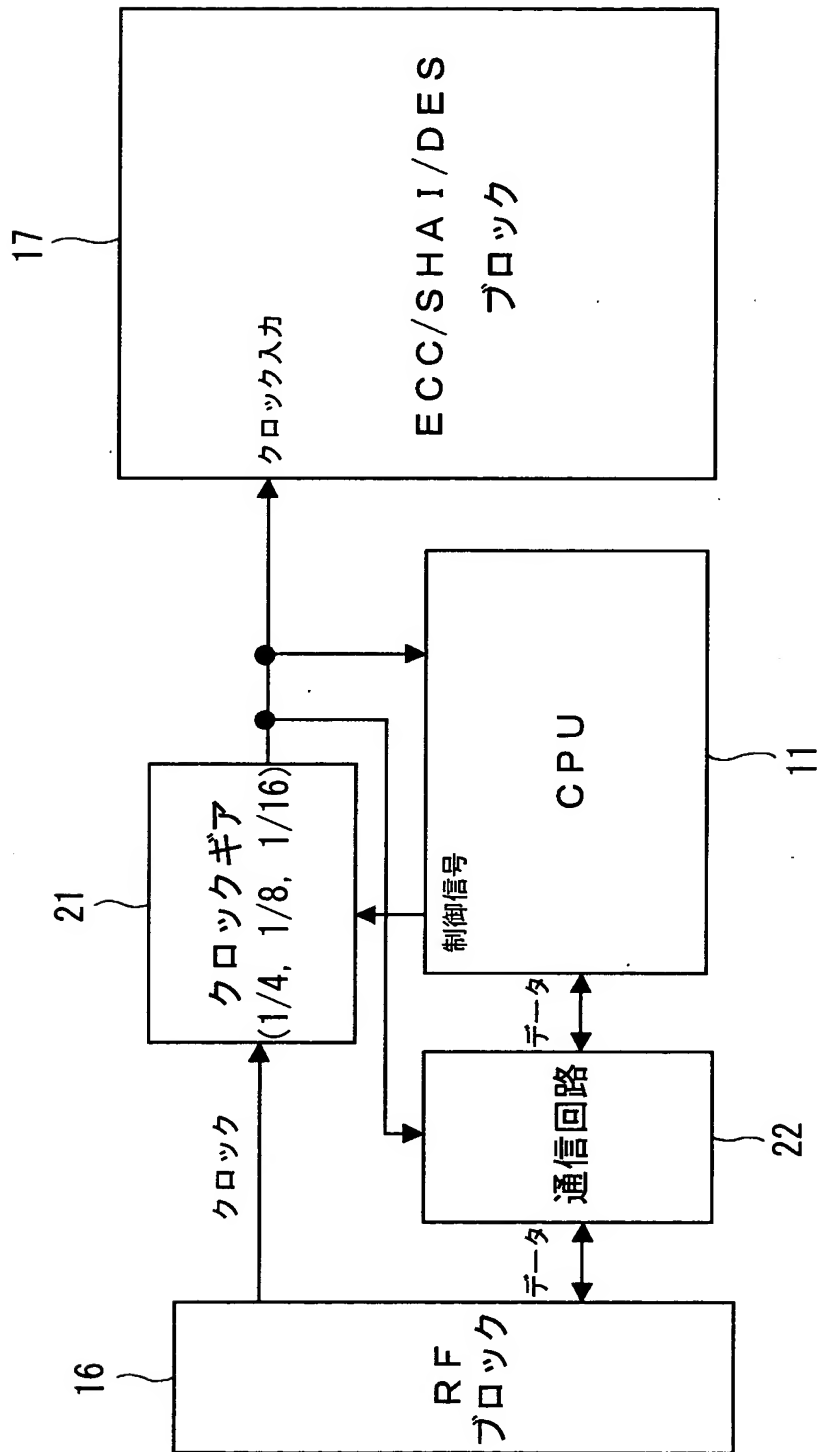
非接触式 IC カードの IC チップの構成ブロック図

【図 5】

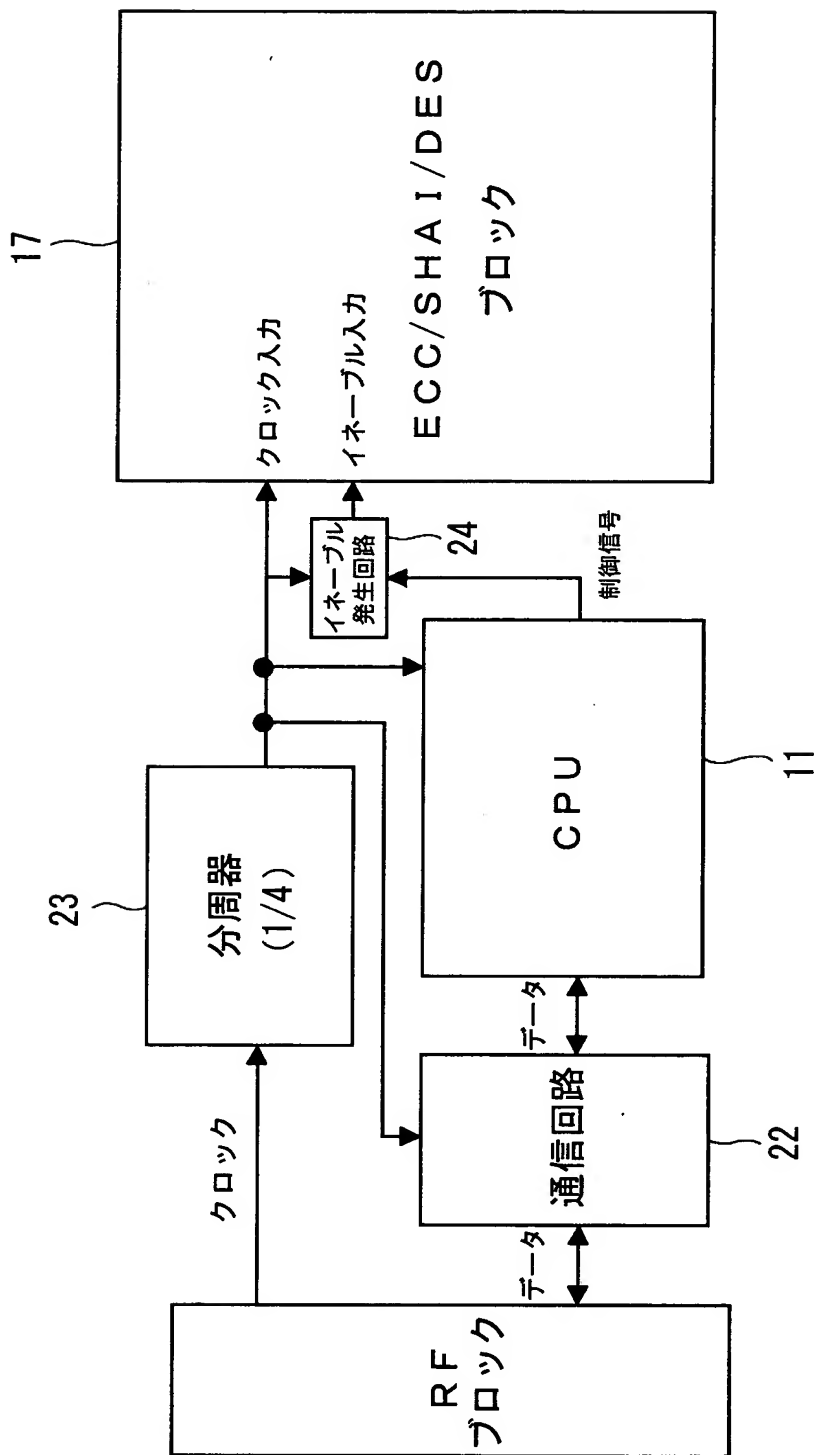


非接触 IC カードの各処理モードにおける動作の説明図

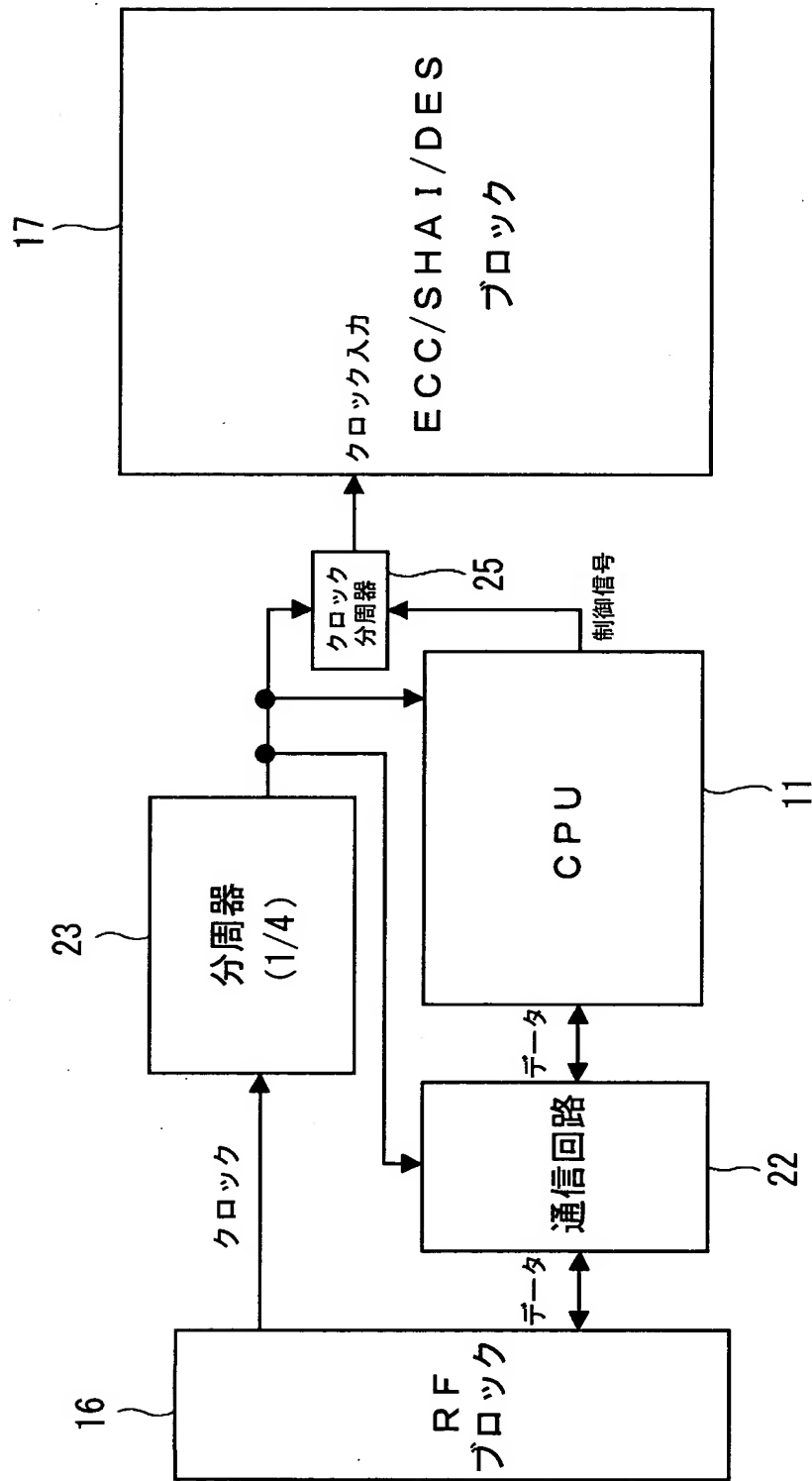
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 公開鍵暗号化方式を採用した場合であっても十分な通信距離を確保し、単一のカードで共通鍵暗号化方式と公開鍵暗号化方式とを両立させ、種々のサービスに適用可能な非接触式 I C カードを提供する。

【解決手段】 公開鍵暗号化方式による暗号化処理を行う D E S ブロック 1 7 ₂ と、共通鍵暗号化方式による暗号化処理を行う E C C / S H A 1 ブロック 1 7 ₁ とを有する暗号化ブロックが I C チップ 4 内に配され、リーダライタとの通信処理と暗号化ブロックにおける各暗号化処理とにおいては、クロックギア 2 1 が内蔵された C P U 1 1 によって動作周波数が変化され、各動作周波数にて動作する。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社
2. 変更年月日 2003年 5月15日
[変更理由] 名称変更
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社